

**CLAIMS**

What is claimed is:

- 1 1. An apparatus comprising:
  - 2 a quotient pre-calculation array (QPA);
  - 3 a main array ; and
  - 4 a quotient pre-calculation circuit, to ensure a true remainder during a following
  - 5 cycle is evenly divisible by a radix.
  
- 1 2. The apparatus of claim 1 wherein the main array and the QPA comprises:
  - 2 a first multiplicand-add multiplexer (MAM) in the main array to couple at least
  - 3 a multiplicand bit with a first carry save adder (CSA) in the main array;
  - 4 a first modulus-add multiplexer (MM) in the QPA to couple at least a modulus
  - 5 bit with a first CSA in the QPA;
  - 6 a second CSA in the main array coupled with the first CSA in the main array
  - 7 and with a first MM in the main array; and
  - 8 a second CSA in the QPA coupled with the first CSA in the QPA, and with a
  - 9 second MM in the QPA.
  
- 1 3. The apparatus of claim 2, wherein the quotient pre-calculation circuit is coupled
  - 2 with the second MM in the QPA, the second MM in the main array, and with the first
  - 3 MM in the QPA.
  
- 1 4. An apparatus as in claim 1, wherein the main array is optimized for area, and
  - 2 the quotient pre-calculation array is optimized for speed.

- 1 5. An apparatus as in claim 2 wherein the CSAs have three inputs, a sum output  
2 and a carry output.
- 1 6. An apparatus as in claim 2 wherein the second CSA in the main array is further  
2 coupled to the first CSA in the QPA through a flip-flop.
- 1 7. An apparatus as in claim 2, wherein the second CSA in the QPA is coupled to a  
2 buffer.
- 1 8. An apparatus as in claim 2, wherein the MAM is coupled to at least one  
2 multiplier bit.
- 1 9. An apparatus as in claim 2 wherein, the second MM in the main array and the  
2 first MM in the QPA are coupled to the quotient pre-calculation array via a flip-flop.
- 1 10. An apparatus as in claim 2, wherein the QPA processes Q bits of a Montgomery  
2 multiplication, and the main array processes N-Q bits of the Montgomery  
3 multiplication.
- 1 11. An apparatus as in claim 10 wherein the main array is Q bits to the left of the  
2 quotient pre-calculation array.
- 1 12. An apparatus comprising:  
2 a quotient pre-calculation array (QPA), an add-one array, and a main array  
3 comprising  
4 a first multiplicand-add multiplexer (MAM) in the main array to couple at least  
5 a multiplicand bit with a first carry save adder (CSA) in the main array;

6 a first modulus-add multiplexer (MM) in the QPA to couple at least a modulus  
7 bit with a first CSA in the QPA;  
8 a first add-one multiplexer (AOM) in the add-one array to couple at least a  
9 binary one bit with a first CSA in the add-one array;  
10 a second CSA in the main array coupled with the first CSA in the main array  
11 and with a first MM in the main array;  
12 a second CSA in the QPA coupled with the first CSA in the QPA, and with a  
13 second MM in the QPA;  
14 a second CSA in the add-one array coupled with the first CSA in the add-one  
15 array, and with a first MM in the add-one array; and  
16 a quotient pre-calculation circuit, to pre-calculate a quotient, coupled with the second  
17 MM in the QPA, the second MM in the main array, and with the first MM in the QPA.

1 13. An apparatus as in claim 12, wherein the first add-one multiplexer is coupled to  
2 at least one multiplier bit via flip-flops.

1 14. An apparatus as in claim 12, wherein the second CSA in the main array is  
2 further coupled to the first CSA in the add-one array, and the second CSA in the add-  
3 one array is coupled to the first CSA in the QPA through one or more flip-flops.

1 15. A method comprising:  
2 adding at least one multiplicand bit from a first multiplicand-add multiplexer in a main  
3 array of a Montgomery multiplier with at least one modulus bit from a first modulus-  
4 add multiplexer in the main array;

5 adding at least one modulus bit from a first modulus-add multiplexer in a quotient pre-  
6 calculation array with at least one modulus bit from a second modulus-add multiplexer  
7 in the quotient pre-calculation array;  
8 pre-calculating the quotient during a first cycle; and  
9 sending at least one value to control the first modulus-add multiplexer in the main  
10 array, the first modulus-add multiplexer in the quotient pre-calculation array, and the  
11 second modulus-add multiplexer in the quotient pre-calculation array so that the value  
12 of the quotient is evenly divisible by the radix during a second cycle through the  
13 Montgomery multiplier.

1 16. A method as in claim 15, further comprising performing an additional cycle  
2 through the Montgomery multiplier to synchronize the bits in the main array and in the  
3 quotient pre-calculation array.

1 17. A method as in claim 15, wherein during the additional cycle the second  
2 modulus-add multiplexer outputs a 0 bit.

1 18. A method as in claim 15 further comprising inserting a 1 bit when necessary to  
2 complete a 2's complement of the multiplicand.

1 19. A method as in claim 15 wherein the first multiplicand-add multiplexer has  
2 values at its inputs consisting at least one of  $-2 \times$  the multiplicand,  $-1 \times$  the  
3 multiplicand,  $0$ ,  $1 \times$  the multiplicand, and  $2 \times$  the multiplicand.

1    20.    An apparatus comprising:  
2                means for adding at least one multiplicand bit from a first multiplicand add  
3    multiplexer in a main array of a Montgomery multiplier with at least one modulus bit  
4    from a first modulus-add multiplexer in the main array;  
5                means for adding at least one modulus bit from a first modulus-add multiplexer  
6    in a quotient pre-calculation array with at least one modulus bit from a second  
7    modulus-add multiplexer in the quotient pre-calculation array;  
8                means for pre-calculating the quotient during a first cycle; and  
9                means for sending at least one value to control the first modulus-add  
10   multiplexer in the main array, the first modulus-add multiplexer in the quotient pre-  
11   calculation array, and the second modulus-add multiplexer in the quotient pre-  
12   calculation array so that the value of the quotient is evenly divisible by the radix during  
13   a second cycle through the Montgomery multiplier.

1    21.    An apparatus as in claim 20, further comprising means for performing an  
2    additional cycle through the Montgomery multiplier to synchronize the bits in the main  
3    array and in the quotient pre-calculation array.

1    22.    An apparatus as in claim 20, wherein the means for pre-calculating the quotient  
2    causes the second modulus-add multiplexer to output a 0 bit during the additional cycle  
3    through the Montgomery multiplier.